



**Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy**



**065.014 Cabinet for Health and Family Services
(CHFS) System Development Life Cycle (SDLC) and
New Application Development Policy**

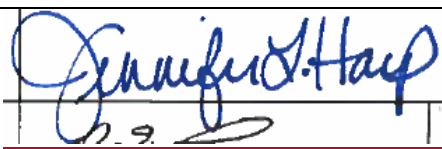

**Version 2.4
April 30, 2019**

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

Revision History

Date	Version	Description	Author
7/20/2010	1.0	Effective Date	CHFS OATS Policy Charter Team
4/30/19	2.4	Review Date	CHFS OATS Policy Charter Team
4/30/19	2.4	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or delegate)	4/30/19	<u>Jennifer Harp</u>	<u></u>
CHFS Chief Information Security Officer (or delegate)	4/30/19	<u>Dennis E. Ceben</u>	<u></u>

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

Table of Contents

1	POLICY DEFINITIONS	4
2	POLICY OVERVIEW	7
2.1	PURPOSE	7
2.1	SCOPE	7
2.2	MANAGEMENT COMMITMENT	7
2.3	COORDINATION AMONG ORGANIZATIONAL ENTITIES	7
2.4	COMPLIANCE	7
3	ROLES AND RESPONSIBILITIES	8
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	8
3.2	CHFS OATS INFORMATION SECURITY (IS) TEAM	8
3.3	CHIEF PRIVACY OFFICER (CPO)	8
3.4	SECURITY/PRIVACY LEAD	8
3.5	CHFS STAFF AND CONTRACTOR EMPLOYEES	8
3.6	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS	8
4	POLICY REQUIREMENTS	9
4.1	GENERAL	9
4.2	NEW APPLICATION DEVELOPMENT	9
5	POLICY MAINTENANCE RESPONSIBILITY	10
6	POLICY EXCEPTIONS	10
7	POLICY REVIEW CYCLE	10
8	POLICY REFERENCES	10

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

1 Policy Definitions

- **Application:** Defined by CHFS as a software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include: Data not releasable under the Kentucky State Law; Protected Health Information; Federal Tax Information; Social Security and Credit Card numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Corrective Action Plan (CAP):** Defined by CHFS as a step by step plan of action that is developed to achieve targeted outcomes for resolution of identified errors in the most cost-effective manner. Defined by IRS Publication 1075 as a report required to be filed semi-annually, detailing the agency's planned and completed action to resolve findings identified through an IRS safeguard review.
- **Critical Systems (Mission Critical):** Defined by CHFS as any production applications developed, maintained or utilized by OATS that have a recovery time objective (RTO) of 7 days or less, a recovery point objective (RPO) based on the backup requirements that are typically nightly or otherwise specified, and/or federally mandated/regulated as critical. These applications are included in the Service Level Agreement (SLA) with COT as "Agency Critical Applications". These applications require creation and maintenance of Business Continuity Plan (BCP), which includes Business Impact Analysis (BIA) and Disaster Recovery Plan (DRP) documents.
- **Database (server or components):** Defined by CHFS as a Database Management System (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.¹³ Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

- Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the IRC and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.
- Oversight Group:** Defined by CHFS as a CHFS comprised group including agency and technical staff that will be a part of communication and movement throughout the System Development Life Cycle (SDLC) process.
- Personally Identifiable Information (PII):** Defined by KRS Chapter 61 House Bill 5 (HB5) and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA).
- Sensitive Data:** Defined by COT standards as data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: All information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth proprietary information including but not limited to intellectual property, financial data and more.
- Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) Security Standards as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

chip0, CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data anything that is inclusive of bank identification/information (i.e. bank routing number, account number, etc.).

- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS.
- **Third Party:** Defined by CHFS as any contracted or government organization that is not a part of the agency's organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs.
- **Threat Modeling:** Defined by CHFS as an engineering technique used to identify threats, attacks, vulnerabilities and countermeasures that could affect your application.
- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Web Server:** Defined by NIST 800-45 Revision 2 as a computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server".

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a system development lifecycle. This document establishes the Cabinet's System Development Life Cycle (SDLC) and New Application Development Policy which helps manage risks and provides guidelines for security best practices regarding software development, and supporting infrastructure that enables projects delivered within schedule, meet compliance regulations, and reduce overall risk to the Confidentiality, Integrity, and Availability (CIA) of Data systems.

2.1 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

2.2 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.3 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.4 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 CHFS OATS Information Security (IS) Team

The CHFS OATS IS Team is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required.

3.3 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.4 Security/Privacy Lead

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of PII, ePHI, FTI and other financial sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS IS Team is responsible for the adherence of this policy.

3.5 CHFS Staff and Contractor Employees

All CHFS contract, state, and vendor staff/personnel must adhere to this procedure. All staff/personnel must comply with referenced documents, found in [Section 8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.6 System Data Owner and System Data Administrators

Management/lead, or appointed delegate, who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

4 Policy Requirements

4.1 General

This policy is established to refine uniform business processes and standards to assure quality development projects are delivered on time and within budget.

Each system or group of related systems will define a methodology for managing Software Development Life Cycle (SDLC). The methodology will consist of the following phases, but is not limited to:

- Initiation
- Threat Modeling
- Development
- Testing
- User Acceptance testing (UAT)
- Implementation
- Maintenance and Operations (M&O)
- Decommissioning

CHFS projects shall use the TFS, or agency other approved system(s), to check code in and out during development or for use in production when required. The OATS IS Team recommends that the code be digitally-signed to maintain integrity between development, integration, test, and production environments.

Each system or group of systems will have an oversight group who will have the responsibility of managing projects and changes in accordance with the SDLC methodology.

Enterprise CIO-082 Critical Systems Vulnerability Assessments Policy states each agency shall engage a third party to assess all critical systems under the agency's responsibility both upon initial implementation into production use and at least every two (2) years thereafter.

These network and server vulnerability assessments do not include the development environments, or application software, related to these systems, which must be tested separately. Each agency shall follow the appropriate notification process outlined in the CHFS Systems Development Lifecycle (SDLC) and New Application Development Procedure prior to conducting these assessments.

4.2 New Application Development

OATS requires all new application development efforts to be reviewed and analyzed. Refer to the CHFS Systems Development Lifecycle (SDLC) and New Application Development Procedure for detailed steps when developing new applications.

065.014 CHFS SDLC and New Application Development Policy	Current Version: 2.4
065.000 Application Development	Review Date: 4/30/2019

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least annually and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Systems Development Lifecycle (SDLC) and New Application Development Procedure
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Information Technology Management Portal (ITMP)
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61: House Bill 5 (HB5)
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-64 Revision 2, Security Considerations in the System Development Life Cycle
- Procurement, Payables, and Asset Tracking System (PPATS)
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)